UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/847,821	05/02/2001	Yoshiaki Sawada	14592	6338

23389 7590 06/19/2003

SCULLY SCOTT MURPHY & PRESSER, PC
400 GARDEN CITY PLAZA
GARDEN CITY, NY 11530

EXAMINER	
TREMBLAY, MARK STEPHEN	
ART UNIT	PAPER NUMBER
2827	

DATE MAILED: 06/19/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action	Application No.	Applicant(s)	
	09/847,821	SAWADA, YOSHIAKI	
	Examiner	Art Unit	
	Mark Tremblay	2876	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 17 March 2003 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE. Therefore, further action by the applicant is required to avoid abandonment of this application. A proper reply to a final rejection under 37 CFR 1.113 may only be either: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114.

PERIOD FOR REPLY [check either a) or b)]

a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
ONLY CHECK THIS BOX WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

1. ☒ A Notice of Appeal was filed on *19 May 2003*. Appellant's Brief must be filed within the period set forth in 37 CFR 1.192(a), or any extension thereof (37 CFR 1.191(d)), to avoid dismissal of the appeal.

2. ☐ The proposed amendment(s) will not be entered because:

   (a) ☐ they raise new issues that would require further consideration and/or search (see NOTE below);

   (b) ☐ they raise the issue of new matter (see Note below);

   (c) ☐ they are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

   (d) ☐ they present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____.

3. ☐ Applicant's reply has overcome the following rejection(s): _____.

4. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

5. ☒ The a)☐ affidavit, b)☐ exhibit, or c)☒ request for reconsideration has been considered but does NOT place the application in condition for allowance because: *see attached*.

6. ☐ The affidavit or exhibit will NOT be considered because it is not directed SOLELY to issues which were newly raised by the Examiner in the final rejection.

7. ☒ For purposes of Appeal, the proposed amendment(s) a)☒ will not be entered or b)☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:

   Claim(s) allowed: *none*.

   Claim(s) objected to: _____.

   Claim(s) rejected: *1-8*.

   Claim(s) withdrawn from consideration: _____.

8. ☐ The proposed drawing correction filed on _____ is a)☐ approved or b)☐ disapproved by the Examiner.

9. ☐ Note the attached Information Disclosure Statement(s)(PTO-1449) Paper No(s). _____.

10. ☐ Other: _____

MARK TREMBLAY
PRIMARY EXAMINER

Response to Arguments

Applicant's arguments filed 3/17/03 have been fully considered but they are not persuasive. Examiner does not agree with Applicant's assertion that Low does not meet all the claim limitations.

In construing the claim language, Examiner is constrained to using the "plain meaning" of the terms, unless the Applicant has defined a new term that lacks an art accepted meaning. In this case, the term "zero-knowledge" has been used. A preferred embodiment has been described. The preferred embodiment is similar to that described by Bruce Schneier in Applied Cryptography, Second Edition, pages 104-105. If Applicant meant to restrict the term "zero-knowledge" to mean an algorithm employing a graph isomorphism, then Applicant would or should have included the term "graph isomorphism" in the claims. This would have raised the particular question of whether a graph isomorphic zero-knowledge credit verifier was anticipated by or obvious over the prior art. Instead, "zero-knowledge" has a broader meaning in the art. Examiner has provided examples of the various ways "zero-knowledge" has been understood in the art. In 1989, Davies and Price seemed to suggest that this term was embodied by the "Fiat-Shamir Protocols" introduced in 1986. (Davies mentions that this protocol is used in smart cards, at page 265). By 1996, Schneier makes clear that several types of "zero knowledge" algorithms exist (Schneier mentions that zero knowledge identification schemes are used in credit cards at page 109). In 1997, Peter Wayner offers a definition of zero-knowledge systems succinctly: "Zero-knowledge proofs are a neat solution for proving that you know something without reavealing any information. This algorithm could be used for a digital cash card to prove it is authentic without revealing its serial number." Also in 1997, Ford and Baum provide a definition of zero knowledge techniques in "Secure Electronic Commerce": "A zero-knowledge technique is a means by which possession of information can be verified without any part of that information being revealed."

The varying definitions of "zero-knowlege" constitute a minor dilemma for the Examiner.

Does Low apply under 35 U.S.C. §102, or not? According to Wayner, and Ford and Baum's definitions, it appears that Low does qualify. Under Davies, and Schneier's more detailed definitions, it does not seem to apply. Thus, the Examiner relied on a 35 U.S.C. §103 combination with Goldwasser as an alternative position. The obviousness of using a zero-knowledge system is supported by Goldwasser, as well as all of the basic texts listed here.

The Applicant's frequent repetition of the term "zero-knowledge" in the arguments does little to persuade the Examiner, since the Applicant avoids discussing the meaning of the term. Also, the assertion that Low's device 245 does not verify the credit card is unpersuasive. As discussed in the interview, from the point of view of the customer and merchant, the device certainly does verify the card. That is the whole point of the device. Examiner does not believe the claims define over this basic function of the device.

Applicant asserts that Low provides a pseudonym which is the equivalent of the credit card account number which could alledgedly be "pilfered" by the business. Examiner strongly disagrees with this reading of Low. Examiner directs the Applicant's attention to the summary of the invention in Low, and to columns 3 and 4. It is clear that even the pseudonym of the customer is encrypted, and never provided to the business S so that the business S can "pilfer" it. Moreover, the pseudonym is not the same as the customer name or the account. That would be like saying the following statements are identical: "The Examiner's name is Mark Tremblay" and "The Examiner's name is 99x488". One statement is true, the other one is false. If the Applicant had no way of colluding with others to find out who is associated with the pseudonym 99x488, even if the Applicant could decrypt the false name, the Applicant would essentially have zero knowledge about the examiner. In the arguments, Applicant appears to miss the fact that Low is describing what appears to be a zero-knowledge technique, where even if the parties conspired to learn the identity of the customer, they could not. The two banks the customer uses do not know each other. See, again, the summary of the invention. This sure sounds like a zero-knowledge system, even if Low doesn't use the term. It appears that Low has invented a novel zero-knowledge technique that was not listed in the text books cited here.

Examiner also finds the arguments presented against the 35 U.S.C. §103 rejection based on Low and Goldwasser unpersuasive. The arguments based on inoperability fail to persuade the

Examiner, because the references are combined at the conceptual level as teachings, not as preferred embodiments. The combined teachings render the claims obvious. There is no requirement that the preferred embodiments be physically combined. Moreover, if the skilled artisan were unable to combine Low and Goldwasser, Examiner would have to doubt whether the skilled artisan could apply the Applicant's generalized example of a zero-knowledge algorithm to the Applicant's own system.

MARK TREMBLAY
PRIMARY EXAMINER

June 13, 2003